



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/668,026	09/21/2000	William T. Jennings	064751.0298	8477
45507	7590	08/18/2006	EXAMINER	
BAKER BOTTS LLP 2001 ROSS AVENUE 6TH FLOOR DALLAS, TX 75201				LAFORGIA, CHRISTIAN A
		ART UNIT		PAPER NUMBER
		2131		

DATE MAILED: 08/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/668,026	JENNINGS, WILLIAM T.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 06 June 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-24 and 26-36 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-24 and 26-36 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____

DETAILED ACTION

1. The amendment of 06 June 2006 has been noted and made of record.
2. Claims 1-24 and 26-36 have been presented for examination.

Response to Arguments

3. Applicant's arguments filed 06 June 2006 have been fully considered but they are not persuasive.
4. In response to the Applicant's arguments that *Elgamal*'s teaching of padding data is not randomization data as required by the claim, the Examiner disagrees, and it is noted that the features upon which applicant relies, such as the importance of the randomization data, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). According to the claim the combination of the token and the randomization data are encrypted. Additionally, randomizing data to be added to a token is unimportant due to the nature of not knowing what data is going to be generated. Furthermore, adding random padding information to keys has been known since at least 09 June 1998 as illustrated by Figures 2-6 and column 9, lines 16-45 of U.S. Patent No. 5,764,772 to Kaufman et al, hereinafter Kaufman.
5. Therefore, *Elgamal* discloses the adding the randomization data as claimed by the Applicant and the rejection is maintained.
6. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching,

suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, motivation for the combination was provided for at column 17, lines 21-40 of Elgamal. If this motivation were found to be insufficient, one of ordinary skill in the art would generally understand the benefits of adding randomized padding data to key information as again taught by Kaufman in column 9, lines 16-45.

7. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

8. See further rejections below.

Claim Rejections - 35 USC § 103

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 1-3, 6-8, 10-12, 14-20, 22-24, 26-30, and 32-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Secure Communications Over Insecure Channels," by Ralph C. Merkle, hereinafter Merkle, in view of U.S. Patent No. 5,825,890 to Elgamal et al, hereinafter Elgamal.

11. As per claims 1, 6, 14, 28, and 33, Merkle teaches creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token; transmitting the set of N trap door encryption-decryption function pairs along with a corresponding token to a receiver', randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token; recording in a key escrow database the created set of N trap door encryption decryption function pairs and the corresponding paired token; recording in the key escrow database the randomly selected trap door encryption decryption function pair along with the encrypted token; and inverting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door encryption-decryption function pair along with the encrypted token to identify the decryption key (pages 296-299).

12. Merkle does not disclose adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair.

13. Elgamal teaches adding padding information to data prior to encrypting the data (column 17, lines 21-40).

14. It would have been obvious to one of ordinary skill in the ad at the time the invention was made to add randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypt the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair, as apposed to sending it back unencrypted as Merkle suggests, since Elgamal discloses at column 17, lines 21-40 that such a modification would allow secure

distribution of information by making the intended data the appropriate length for block ciphers, as well as provide a method for the receiver to detect whether the data has been tampered with. Furthermore, adding random padding information to keys has been known since at least 09 June 1998 as illustrated by Figures 2-6 and column 9, lines 16-45 of Kaufman.

15. As per claims 2 and 29, Merkle teaches encrypting the created set of N trap door encryption-decryption function pairs and the randomly selected trap door function along with the decryption key prior to recording in the key escrow database (page 298).

16. As per claims 3, 7, 14, 30 and 36, Merkle does not explicitly teach the receiver selecting more than one of the puzzles to decrypt. Clearly from the teachings of Merkle one of ordinary skill in the art would know that the work needed to be performed by an eavesdropper plotting to learn the decryption key is $O(n^2)$. Having the receiver choose more than one puzzle slightly increases the poor security of Merkle's system by forcing the eavesdropper to perform more calculations (page 299).

17. As per claim 8, Merkle teaches decrypting the cryptogram of a cryptogram/decryption key pair using the associated decryption key to identify token information (page 299).

18. As per claim 10, Merkle teaches the utilization of a symmetrical cryptosystem (page 296).

19. As per claim 11, Merkle teaches the utilization of a public key cryptosystem (page 299).

20. As per claims 12 and 35, Merkle teaches wherein recording in an escrow database further comprises encrypting the generated set of N cryptogram/decryption key pairs and a response message from the receiver prior to recording (page 296).

21. As per claim 15, Merkle teaches decrypting at the receiver the cryptogram to identify the corresponding token utilizing the decryption key of the cryptogram/decryption key pair (page 296).

22. As per claims 16 and 32, Merkle teaches encrypting at the receiver an escrow key comprises generating a cryptogram comprising', the corresponding token, the decryption key and randomization information (page 298).

23. As per claim 17, Merkle teaches decoding the encrypted escrow key comprises selecting a decryption key randomly from a selected group of decryption keys (page 296).

24. As per claim 18, Merkle teaches comprising recognizing a correct decoding result utilizing structural information embedded in the response message (page 296).

25. As per claim 19, Merkle teaches creating at an originator further comprises generating the set of N trap door functions utilizing a selected encryption function and a private encryption key (page 297).

26. As per claims 24 and 34, Merkle does not explicitly teach the receiver selecting more than one of the puzzles to decrypt. Clearly from the teachings of Merkle one of ordinary skill in the art would know that the work needed to be performed by an eavesdropper plotting to learn the decryption key is $O(n^2)$. Having the receiver choose more than one puzzles slightly increases the poor security of Merkle's system by forcing the eavesdropper to perform more calculations. Merkle teaches encrypting at the receiver an escrow key comprises generating a cryptogram comprising', the corresponding token, the decryption key and randomization information (page 298).

27. As per claim 23 and 25, Merkle teaches the utilization of a symmetrical cryptosystem (page 296).

28. As per claim 24, Merkle teaches the utilization of a public key cryptosystem (page 299).

29. As per claim 26, Merkle teaches recording in an escrow database the created N trap door functions along with each corresponding token and the encrypted escrow key with the randomly selected trap door function (page 298).

30. As per claim 27, Merkle teaches inverting the recorded set of N trap door functions and the encrypted escrow key with the randomly selected trap door function to identify a decryption key from the key escrow database (page 297 and 298).

31. Claims 4, 5, 9, 13, 21, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Merkle in view of Elgamal as applied above, and further in view of U.S. Patent No. 5,815,573 to Johnson et al., hereinafter Johnson.

32. As per claims 4, 5, 31 Merkle teaches using identifying information to distinguish when puzzles have been correctly solved (page 296).

33. Merkle and Elgamal do teach the use of a digital signature. Merkle does teach that keys are looked up based upon a user (page 298). Therefore there is a need to have a positively identifying means to ascertain the correct author of a published key.

34. Johnson teaches the use of a digital signature (column 10, lines 61-63). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Johnson et al within the combined system of Merkle and Elgamal because it would associate a key to a user with provable certainty.

35. As per claim 9, Merkle and Elgamal do not teach explicitly using a linear transformation to combine the token information.

36. Johnson teaches the use of linear transformation to add keys together (figure 1, element 110). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Johnson within the combined system of Merkle and

Elgamal because linear transforms are a fast well established operation in order to carry out transformations.

37. As per claims 13 and 21, Merkle teaches using identifying information to distinguish when puzzles have been correctly solved (page 296).

38. Merkle and Elgamal do teach the use of a digital signature. Merkle does teach that keys are looked up based upon a user (page 298). Therefore there is a need to have a positively identifying means to ascertain the correct author of a published key.

39. Johnson teaches the use of a digital signature (column 10, lines 61-63).

40. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Johnson with the combined system of Merkle and Elgamal because it would associate a key to a user with provable certainty.

Conclusion

41. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

42. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2131

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

43. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

44. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

45. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

CHRISTOPHER REVAK
PRIMARY EXAMINER

Cll 8/16/06